Amendments to the Specification:

Before paragraph [0002] please insert the heading: "**BACKGROUND OF THE INVENTION**."

Please amend paragraph [0002] as follows:

[0002] The amount of data that may be stored on portable digital devices is rapidly increasing, and likewise data transfer speeds are continually increasing such that there is significant scope for visitors to premises to engage in unauthorized and surreptitious downloading of material from an unsecured[[.]] PC or terminal. Furthermore, the ongoing development of communications such as 2.5G and 3G (and future generation) technology will provide extremely fast data transfer speeds (typically 144kb/sec to 2Mb/sec) to give transfer speeds similar to current "broadband" technology to mobile users. This opens up many new applications and it is envisaged that integrated devices will be used which combine the functionality of a mobile (cell) phone with that of a camera capable of taking still or moving images. This in turn creates numerous opportunities but also carries with it some risk. For example, making devices widely available which are capable of capturing and transmitting good still or movie images and/or sound recordings may compromise security in many applications. For example, a legitimate visitor in a commercial premises could surreptitiously record and transmit still or movie images of a sensitive commercial nature, for example images of documents, building layout, industrial processes etc. Elsewhere, in public premises such as museums, theatres, concert halls, etc. a visitor may surreptitiously capture and[[.]] transmit still or movie images or music performances or the like in contravention of their contractual obligations, copyright law, etc. Concerns have also been expressed at the possibility of images of children or adults being covertly taken in locker rooms etc. and there are also religious objections to the unauthorized capture of images of people. These concerns need to be addressed by the service providers and manufacturers if the technology is not to run into problems.

Before paragraph [0003] please insert the heading: "**SUMMARY OF THE INVENTION**."

Please amend paragraph [0008] as follows:

[0008] The geographic location may be monitored in numerous ways. In one example the portable digital device may have a navigation module or functionality such as GPS + GSM, GPRS, CDMA, UTMS and 3G). Alternatively, where the portable digital device operates within a cellular network, the location of the portable digital device may be determined by triangulation of signals from two or more cellular base stations. The system may utilize a local transmitter to increase the overall reception. Where the prohibited zone is in an area accessible only through selected entry points, each entry point may have an induction loop or other detector designed to detect when a portable digital device enters the prohibited zone through said entry point. Other means of detection include infrared signaling and short range low power radio systems such as WL4N, Wi-fi and Bluetooth. Each of the above systems preferably detects not only the presence of the portable digital device but also an information address such as the mobile telephone number uniquely to identify the portable digital device. It will be appreciated that GPS does not normally work in buildings as it requires a line of sight, and so a GPS system may be more appropriate for large out of doors prohibited zones such as airfields etc. For use inside a building the system may be modified, for example, by placing a GPS antenna on the[[.]] building so that the location of the building is determined and the disabling signal passed to relevant rooms within the building and then broadcast by e.g. an IR or radio transmitter.

Please amend paragraph [0014] as follows:

[0014] The inhibition operation may be communicated to the portable digital device by a number of ways; for example it may make use of the SMS text messaging system or a software change downloaded by the network operator, i.e. a "SIM update". Alternatively, the signal to the portable digital device to inhibit the operation may be transmitted over one or more radio frequencies, e.g. the signal may be sent using frequencies supported by one or more of GSM, GPRS, 3G, I-Mode, UTMS, Ultrawideband (UWB) wireless data standard and/or CDMA or the like. This can allow the method to work over more than one network. The one or more frequencies may include a "license-free[[.]] frequency" and/or a FM/AM radio frequency. The one or more frequencies used to transmit the signal may be changed at intervals to help improve security. Further, the signal may be transmitted in the form of an audio signal/tone, typically one having a frequency outside normal human hearing range. The tone may or may not be encrypted and can be decrypted at the device if needed. The signal may be transmitted at one or more optical frequencies (fixed or modulated), e.g. infrared or ultra-violet frequencies. The device may be provided with an optical receiver, which may be integral with or separate from the device.

Please amend paragraph [0015] as follows:

[0015] The method may further include a step of installing code on the device for performing the control of usage of the device. The usage control code may be installed by means of being included in a memory, processor or another component (e.g. a SIM card) within the device.

Please amend paragraph [0051] as follows:

[0051] Referring initially to Figure 1, there is shown a prohibited zone 10, here in the form of a room, where it is required to prevent operation of a camera or video image capture device 12 on a portable digital device 14. In this embodiment the portable digital device 14 is designed such that, on receipt of a predetermined signal, a circuit 16 inhibits operation of the imaging device 12. This could be by preventing any image capture at all or preventing transmission of an image once captured. In this embodiment the circuit 16 is responsive to an inhibit signal emitted from a low range transmitter 18 located just inside the door into the prohibited zone 10. On leaving the room the camera/video functionality may be restored by transmitting a further signal (not shown) to enable the circuit 16. In this arrangement it is not necessary to determine the position of' the portable digital device 14 absolutely because the prohibited zone is accessible through just one access point and so the system only needs to know whether the communication device[[.]] has been brought in to or out of the zone 10.

Please amend paragraph [0055] as follows:

[0055] Referring now to Figure 5, this embodiment of device employs "Bluetooth" technology to inhibit operation of a camera module forming part of a mobile (cell) phone. The commercial range of mobile phones is continually evolving but current typical popular camera phone devices include Nokia 3650 and 7650, Sony Ericcson P800, Samsung SGH-V205, Samsung V200, Sanyo SCP-5300 and Sharp GX10i. There are two main components in this embodiment, namely a camera-phone camera. application and a PC application. The camera-phone camera application is a simple picture-taking application that also advertises a new Bluetooth service called "camera restrictor" which is discoverable by a remote device during a Bluetooth discovery routine. The PC application is typically a Windows application (though other types of operating system are not excluded) that uses a Bluetooth stack suite of programs to perform a device enquiry to identify Bluetooth devices in range and to send messages[[.]] to those devices that advertise the "camera restrictor" service during the Bluetooth discovery routine, to disable the picture-taking application.

Please amend paragraph [0056] as follows:

[0056] The camera application on the phone and the PC application communicate via a serial connection over Bluetooth. The PC application requires no input from the user - it only displays information about the Bluetooth devices that are within range of the PC, and connects automatically to those devices which are advertising the "camera restrictor" service. The camera application allows the[[.]] user to take photographs (but these are not stored on the device). The user does not control the restricting functionality, but when the camera is restricted (by having received a disabling signal from the PC application) messages are displayed to indicate when the last restricting message was received, and when the restriction is to be lifted (assuming no more messages are received at that time). The restrictor application shown on the top left of Figure 5 is a Windows application that uses the Bluetooth stack (typical examples are the stack included in the Windows XP Platform SDK, or the Widcomm stack) to enumerate all Bluetooth devices in range and the services they offer. Once it has finished detecting devices, it connects to each device that advertises a "camera restrictor" service in turn, and sends a simple serial message. The application continuously loops around these actions, detecting devices in range, and then connecting and sending data to those that advertise the "camera restrictor" service. The restrictor application may have the ability to monitor/report upon the number of devices within a restricted area.

Please amend paragraph [0063] as follows:

[0063] It should be appreciated that where the area within which picture taking is to be inhibited is relatively large, several PCs may be set up to provide extended[[.]] area coverage, each working in a similar manner to that described above.

Please amend paragraph [0068] as follows:

[0068] Figure 7 illustrates steps that can be performed by an embodiment of the functionality-restriction software executed on the portable digital device. The software is ideally the only way to access to the camera functionality of the device so that the functionality-restriction software cannot be bypassed by using another software application on the device. In the example, the device comprises a mobile camera phone having Bluetooth™ capabilities. The process starts at step 700 and then at step 702 the camera advertises that it is configured with the camera restrictor software using known[[.]] Bluetooth™ techniques. For example, the camera restrictor software can be advertised as a Bluetooth (TM) serial port class service with a unique identifier (UID) of Ox100513$B. Whenever character data is received via this port, the software can switch the device to its restricted mode of operation.

Please amend paragraph [0073] as follows:

[0073] Turning to Figure 8, the process performed by the server component commences at step 800 and at step 802 the server searches for Bluetooth ™ devices within the restricted zone. At step 804 a check is carried out as to whether the search is complete. If the check is not complete then at step 806 a question is asked as to whether a new device has been found. If this is answered in the negative then control is passed back to step 804. If a new device was found at step 806 then control is passed to step 808 where the found device is added to the list of known devices stored by the server: Data regarding the device class, the device user identifier and device friendly name may be stored. The server component may display this information to a user at a security monitoring station by means of a standard control list which presents a grid or spreadsheet style of view. In this way, the user can quickly ~~examiner~~ examine the list of known devices in range and see which devices are configured with the camera restriction software and which of those currently inactive are unable to take any pictures. Steps 802 to 808 can be thought of as a "discovery cycle" of the process and the remaining steps can be thought of as a "restrict cycle ".

Please amend paragraph [0078] as follows:

[0078] In the above embodiments, a suitably equipped PC may upload software so that it may operate as a base station in a protected area, and the invention extends to a program for controlling a suitably configured computer to operate as a base station. Likewise the software could be loaded onto a wireless gateway, so that the wireless gateway also acted as a base station. Methods of loading appropriate system software onto the mobile device are discussed in the section[[.]] "Methods for installing software/hardware to the client" below.

Methods for communication with the client device (phone handset, pda etc) to disable the camera or other data capture application

Before paragraph [0081], please amend heading as follows:

Radio[[.]] Transmission at License-free frequencies

Please amend paragraph [0089] as follows:

[0089] The software component of the. system could be available within the operating system of the client. Current examples include Symbian, Microsoft Smartphone[[.]] OS and manufacturer specific operating systems.

Please amend paragraph [0098] as follows:

[0098] Sometimes, situations may arise whereby a noncompliant handset (i.e. without some or all of the software for implementing the system discussed herein) is used to take surreptitious images in a protected area (i.e. nodes installed and secure zone created). In this situation, a further set of security measures can be included. These measures seek to confiscate the image once it has been taken and an attempt is made to transfer it over a network, e.g. a GSM network and or ~~ISP's~~ ISPs (if sent via Internet). The network may be configured to filter and confiscate the image and alert relevant authorities, e.g. employer, police. The system can use audio and/or visual techniques. In the audio form, the node emits an encrypted tone or “watermark” that is captured within the data recording session but is inaudible to the human ear. Once sent via GSM or the Internet, the relevant filters recognize that the audio file had been recorded surreptitiously in a designated secure zone and "pull it back" or confiscate. At this stage, the network provider or ISP can inform the coordinator of the designated secure zone that an individual with a particular phone number took a particular recording[[.]] in this secure zone and that particular time.

Please amend paragraph [0100] as follows:

[0100] In a situation whereby a phone does have the relevant disabling functionality, but the GSM, Bluetooth or other communication methods are malfunctioning[[;]], the system may need to use a secondary method to stop the image being sent. The system may need to have the ability to confiscate/delete watermarked images and/or audio and possibly alert the network provider.

Please amend paragraph [0101] as follows:

Node infrastructure used to communicate messages to clients in particular area

[0101] ~~Node infrastructure used to communicate messages to clients in particular area~~ The infrastructure represented by the system uses nodes to communicate with compliant clients. This creates a wireless network within a particular area. This network can be utilized further to disseminate particular information to individuals using the client. One example could be in offices whereby pertinent information such as times of upcoming practice fire alarms are sent to the client with corresponding details of the nearest fire exits. Similarly, the network could be used as a[[.]] direct marketing tool in shopping malls whereby shop locations and special offers can be communicated to the client once it enters the shopping area or zone. Other examples include the streaming of film clips in cinema foyers.

Please amend paragraph [0102] as follows:

[0102] Some high end handsets, for example Handspring Treo, can take photo images even when its core communication method (e.g. GSM) is turned off. In this situation, the system can be further enhanced in a number of ways. Firstly, the software ensures that even if the GSM functionality is turned off, other methods of communication are still available to disable the camera's use e.g. Bluetooth (TM), infra-red, WI-Fl and so forth. Secondly, the system and corresponding software can force the camera functionality to be disabled as standard once radio communication has been switched off. Thirdly, the system could be incorporated into the client software such that it transmission is disabled if it has photo attachments whilst in the privacy zone.

MP3 players and USB portable drives

Increasingly, MP3 players like the "ipod" and other portable drives have the ability to store images[[.]] and record audio. The aforementioned system could cover these devices also, stopping recording in protected locations.

Please modify the abstract as follows:

A system for controlling usage of a portable digital device having an audio [[5]] and/or image data recording or capture function. Operation of the data recording or capture function is inhibited when the portable digital device is located in a specific geographic region.